PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-024875
(43)Date of publication of application : 26.01.2001

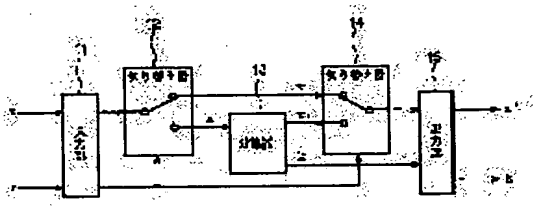
(51)Int.Cl. H04N 1/387
G06T 1/00
G09C 5/00
H04N 5/92
H04N 7/167

(21)Application number : 11-193331
(22)Date of filing : 07.07.1999

(71)Applicant : CANON INC
(72)Inventor : HAYASHI JUNICHI

(54) METHOD AND DEVICE FOR IMAGE PROCESSING AND STORAGE MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To output image data in which a watermark image is embedded and information eliminated for embedding it as key information by changing pixel information for original image data included in an area instructed by form information of the watermark image, generating key information decided based on the pixel information and outputting the changed original image data and the key information.
SOLUTION: In an electronic watermark embedding device, original image (x) each of which includes plural pixels constituted with a pixel position and a pixel value and an embedded image (r) of watermark image data consisting of the pixel position for indicating a form of an image to be embedded are inputted to an input part 11. In a separator 13, at least more than one color component is separated from the original image (x) out of three color components composing the pixel value of the specified pixel position of the original image (x) from a switching device 12, and the separated information is stored as key information (k). Also, remaining information x1 from which this key information (k) is separated is outputted to a switching device 14.



LEGAL STATUS

[Date of request for examination] 06.10.2003
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

CLAIMS

[Claim(s)]
[Claim 1] An input means to be the image processing system which spaces through subject-copy image data and embeds an image, and to input the configuration information on subject-copy image data and said watermark image, A modification means to change the pixel information on said subject-copy image data contained in the field directed for said configuration information, The image processing system characterized by having an output means to output a key information generation means to generate the key information determined based on the pixel information changed by said modification means, and the subject-copy image data, by which pixel information was changed by said modification means and said key information.
[Claim 2] Said modification means is an image processing system according to claim 1 characterized by changing the value of the predetermined color component of the pixel value of the pixel location which compares said configuration information with each pixel location of said subject-copy image data, and is included in said configuration information.
[Claim 3] Said modification means is an image processing system according to claim 1 characterized by changing a part of pixel value of the pixel location which compares said configuration information with each pixel location of said subject-copy image data, and is included in said configuration information.
[Claim 4] Said key information generation means is an image processing system given in claim 1 characterized by generating said key information based on the difference of said changed pixel information and the pixel value to which said subject-copy image data correspond thru/or any 1 term of 3.
[Claim 5] Said output means is an image processing system given in claim 1 characterized by having an encryption means to encipher said key information thru/or any 1 term of 4.
[Claim 6] Said output means is an image processing system given in claim 1 characterized by having a compression means to compress said key information thru/or any 1 term of 5.
[Claim 7] It is the image processing system with which it spaced through subject-copy image data, and the image was embedded and which embeds, inputs image data and restores said subject-copy image data. Said embedding image data, A restoration means to restore the pixel information on said embedding image data contained in the field instructed to be an input means to input the configuration information and key information on said watermark image for said configuration information to the pixel information on original based on said key information, The image processing system characterized by having an output means to output subject-copy image data including the pixel information restored by said restoration means.
[Claim 8] Said restoration means is an image processing system according to claim 7 characterized by changing the value of the predetermined color component of the pixel value of the pixel location which compares said configuration information and each pixel location of said embedding image data, and is included in said configuration information according to said key information.
[Claim 9] Said restoration means is an image processing system according to claim 7 characterized by changing a part of pixel value of the pixel location which compares said configuration information and each pixel location of said embedding image data, and is included in said configuration information according to said key information.
[Claim 10] Said key information is an image processing system given in claim 7 characterized by having further a decryption means to be enciphered and to decode the key information concerned thru/or any 1 term of 9.
[Claim 11] Said key information is an image processing system given in claim 7 which the data compression is carried out and is characterized by having further an expanding means to elongate the key information concerned thru/or any 1 term of 10.
[Claim 12] The input process which is the image-processing approach which spaces through subject-copy image data and embeds an image, and inputs the configuration information on subject-copy image data and said watermark image, The modification process which changes the pixel information on said subject-copy image data contained in the field directed for said configuration information, The image-processing approach characterized by having the output process which outputs the key information generation process which generates the key information determined based on the pixel information changed at said modification process, and the subject-copy image data with which pixel information was changed at said modification process and said key information.
[Claim 13] The image-processing approach according to claim 12 characterized by changing the value of the predetermined color component of the pixel value of the pixel location which compares said configuration information with each pixel location of said subject-copy image data, and is included in said configuration information at said modification process.
[Claim 14] The image-processing approach according to claim 12 characterized by changing a part of pixel value of the pixel location which compares said configuration information with each pixel location of said subject-copy image data, and is included in said configuration information at said modification process.
[Claim 15] The image-processing approach given in claim 12 characterized by generating said key information at said key information generation process based on the difference of said changed pixel information and the pixel value to which said subject-copy image data correspond thru/or any 1 term of 14.
[Claim 16] Said output process is the image-processing approach given in claim 12 characterized by having the encryption process which enciphers said key information thru/or any 1 term of 15.
[Claim 17] Said output process is the image-processing approach given in claim 12 characterized by having the pressing operation which compresses said key information thru/or any 1 term of 16.
[Claim 18] It is the image-processing approach by which it spaced through subject-copy image data, and the image was embedded and which embeds, inputs image data and restores said subject-copy image data. Said embedding image data, The restoration process which restores the pixel information on said embedding image data contained in the field instructed to be the input process which inputs the configuration information and key information on said watermark image for said configuration information to the pixel information on original based on said key information, The image-processing approach characterized by having the output process which outputs subject-copy image data including the pixel information restored

at said restoration process.
[Claim 19] The image-processing approach according to claim 18 characterized by changing the value of the predetermined color component of the pixel value of the pixel location which compares said configuration information and each pixel location of said embedding image data, and is included in said configuration information at said restoration process according to said key information.
[Claim 20] The image-processing approach according to claim 18 characterized by changing a part of pixel value of the pixel location which compares said configuration information and each pixel location of said embedding image data, and is included in said configuration information at said restoration process according to said key information.
[Claim 21] Said key information is the image-processing approach given in claim 18 characterized by having further a decryption means to be enciphered and to decode the key information concerned thru/or any 1 term of 20.
[Claim 22] Said key information is the image-processing approach given in claim 18 which the data compression is carried out and is characterized by having further the expanding process which elongates the key information concerned thru/or any 1 term of 21.
[Claim 23] The input process module which is the storage which memorizes the program which performs the image-processing approach which spaces through subject-copy image data and embeds an image, and inputs the configuration information on subject-copy image data and said watermark image, The modification process module which changes the pixel information on said subject-copy image data contained in the field directed for said configuration information, The storage characterized by having the output process module which outputs the key information generation process module which generates the key information determined based on the pixel information changed at said modification process, the subject-copy image data with which pixel information was changed at said modification process, and said key information.
[Claim 24] It is the storage which memorized the program which performs the image-processing approach by which it spaced through subject-copy image data, and the image was embedded, and which embeds, inputs image data and restores said subject-copy image data. Said embedding image data, The input process module which inputs the configuration information and key information on said watermark image, The restoration process module which restores the pixel information on said embedding image data contained in the field directed for said configuration information to the pixel information on original based on said key information, The storage characterized by having the output process module which outputs subject-copy image data including the pixel information restored at said restoration process.

[Translation done.]

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the image-processing approach and equipment which generate the image data which embedded digital watermarking to subject-copy image data, and attain to them, or remove a digital-watermarking part from the image data, and generate subject-copy image data, and a storage.
[0002]
[Description of the Prior Art] The digital image which treats an image as a digital signal has the descriptions, like even if it can copy easily and moreover performs such a copy by computer etc. as compared with the analog image expressed with the conventional analog signal, image quality does not deteriorate, and has the advantage that it can moreover transmit to a remote place without degradation of image quality through a communication line. However, a digital image has the problem of it being easily copied illegally by the third person and redistributing, according to such a description. There is technique called digital watermarking to one of the approaches for preventing this.
[0003] It roughly classifies into this digital watermarking, and there is a visible mold which forms the invisible mold which embeds watermark information, such as copyright information and User Information, in an image in the form which is not a foregone conclusion, and watermark images, such as a LOGO of the firm which holds that copyright, on that image in the form which is a foregone conclusion. In digital watermarking of the former invisible mold, it cannot recognize that watermark information is embedded only by glancing at the embedding image. Therefore, although deletion of watermark information is hard to be performed, the illegal copy of the image and unjust edit are easy to be performed compared with the case of a visible mold. However, since it spaced into the digital image data and information remains even when metaphor digital image data is copied or edited unjustly, the user who performed the unjust copy etc. can be specified by the user ID embedded as watermark information.
[0004] After performing frequency conversion, such as a fast Fourier transform, a discrete cosine transform, and wavelet transform, to an input image as a typical thing of digital watermarking of such an invisible mold, spacing through a frequency domain and adding information, the technique of performing embedding of digital watermarking is mentioned by performing reverse frequency conversion. Among these, by the technique by the fast Fourier transform, after an input image added and diffuses PN sequence, it is divided into a block, the Fourier transform is performed for every block, and 1-bit watermark information is embedded at 1 block. In this way, an inverse Fourier transform is given to the block with which it spaced and information was embedded, the again same PN sequence as the beginning is added, and it becomes a synthetic image. This technique is detailed by the "watermark signing method to the image by PN sequence" (1997, code, information security symposium lecture collected works, SCIS97-26B) by Onishi, **, Matsui, etc. Moreover, the technique by the discrete cosine transform is divided into a block, and carries out a discrete cosine transform for every block. After embedding 1-bit information at 1 block, inverse transformation is carried out and a synthetic image is generated. This is detailed to "the digital-watermarking method in the frequency domain for the protection of copyrights of a digital image" (1997, the code, information security symposium lecture collected works, SCIS97-26A) by Nakamura, the brook, Takashima, etc. Furthermore, the technique by wavelet transform is technique to twist the need of carrying out block division of the input image, and is detailed to "experimental consideration about the safety and dependability of the electronic watermark technique using wavelet transform" (1997, the code, information security symposium lecture collected works, SCIS97-26D) by Ishizuka, Sakai, Sakurai, etc. [of this] Moreover, there is also the technique (Digimarc, U.S. Pat. No. 5,636,292, etc.) of calculating to the hue of a pixel, lightness, etc. and embedding digital watermarking.
[0005] On the other hand, in digital watermarking of a visible mold, since watermark information is written in on the digital image in the form which is in sight by the eye, if it remains as it is, it uses, and it is hot and effective in considering an illegal copy and unjust edit and stopping them. Such visible mold digital watermarking may be constituted so that it may be possible only for a right user to space completely and to remove information. As the example, to the user who is not the normal of the image data, the image with which the watermark of a visible mold was embedded is distributed, and the case where the image with which the watermark of a visible mold is not embedded is distributed can be considered to the user of normal.
[0006] As one approach for realizing this, the method which distributes the image data which sticks copyright information on subject-copy image data, and stuck the LOGO etc. to the user who is not regular, and distributes subject-copy image data as it is to the user of normal has been used by replacing the pixel value of images, such as a LOGO, with the pixel value of a subject-copy image conventionally. However, since the contents of the part of the image data which embedded digital watermarking of a visible mold are transposed to the contents of the images, such as a LOGO, a user cannot know the contents of the subject-copy image data corresponding to this part. Furthermore, in order to remove such digital watermarking, all the subject-copy image data needed to be transmitted, but generally, since subject-copy image data were very big data, much time amount was needed for transmitting this.
[0007] Moreover, with this, there is also another method proposed by JP,8-241403,A. This is a method which saves a chromaticity and embeds digital watermarking of a visible mold by carrying out linear transformation of the brightness value of subject-copy image data. By this method, although the user was able to get to know the contents of the subject-copy image data of the field where digital watermarking of a visible mold was embedded, the approach of canceling digital watermarking of a visible mold is not clarified.
[0008]
[Problem(s) to be Solved by the Invention] It is not proposed about the approach of canceling a digital-watermarking part of the image data where digital watermarking of a visible mold was conventionally embedded to subject-copy image data as explained above, and the digital watermarking was embedded. For this reason, in order to offer the subject-copy image data of which digital watermarking of a visible mold was canceled to the user of normal, all the data of that subject-copy image

needed to be transmitted to that user. Transmission of such all subject-copy image data required much time amount, and had become a problem also in respect of the transmission cost.
[0009] This invention was made in view of the above-mentioned conventional example, is spaced with subject-copy image data, inputs the configuration information on an image, and it aims at offering the image-processing approach and equipment which output the image data where the watermark image was embedded, and the information removed in order to embed the watermark image as key information.
[0010] Moreover, the purpose of this invention is to offer the image-processing approach and equipment which restore data for a subject-copy image based on the image data where the watermark image was embedded, and the key information corresponding to the information removed in order to embed the watermark image.
[0011] Furthermore, the purpose of this invention spaces with subject-copy image data, inputs the configuration information on an image, makes key information the image data where the watermark image was embedded, and information removed in order to embed that watermark image, compresses this key information, and reaches further, or aims at offering the image-processing approach and the equipment which are enciphered and outputted.
[0012] Moreover, the purpose of this invention is to offer the image-processing approach and equipment corresponding to the image data where the watermark image was embedded, and the information removed in order to embed the watermark image which restore data for a subject-copy image based on the key information which compressed, reached or was enciphered.
[0013]
[Means for Solving the Problem] In order to attain the above-mentioned purpose, the image processing system of this invention is equipped with the following configurations. Namely, an input means to be the image processing system which spaces through subject-copy image data and embeds an image, and to input the configuration information on subject-copy image data and said watermark image, A modification means to change the pixel information on said subject-copy image data contained in the field directed for said configuration information, It is characterized by having an output means to output a key information generation means to generate the key information determined based on the pixel information changed by said modification means, and the subject-copy image data, by which pixel information was changed by said modification means and said key information.
[0014] In order to attain the above-mentioned purpose, the image processing system of this invention is equipped with the following configurations. It is the image processing system with which it spaced through subject-copy image data, and the image was embedded and which embeds, inputs image data and restores said subject-copy image data. Namely, said embedding image data, A restoration means to restore the pixel information on said embedding image data contained in the field instructed to be an input means to input the configuration information and key information on said watermark image for said configuration information to the pixel information on original based on said key information, It is characterized by having an output means to output subject-copy image data including the pixel information restored by said restoration means.
[0015] In order to attain the above-mentioned purpose, the image-processing approach of this invention is equipped with the following processes. Namely, the input process which is the image-processing approach which spaces through subject-copy image data and embeds an image, and inputs the configuration information on subject-copy image data and said watermark image, The modification process which changes the pixel information on said subject-copy image data contained in the field directed for said configuration information, It is characterized by having the output process which outputs the key information generation process which generates the key information determined based on the pixel information changed at said modification process, and the subject-copy image data with which pixel information was changed at said modification process and said key information.
[0016] In order to attain the above-mentioned purpose, the image-processing approach of this invention is equipped with the following processes. It is the image-processing approach by which it spaced through subject-copy image data, and the image was embedded and which embeds, inputs image data and restores said subject-copy image data. Namely, said embedding image data, The restoration process which restores the pixel information on said embedding image data contained in the field instructed to be the input process which inputs the configuration information and key information on said watermark image for said configuration information to the pixel information on original based on said key information, It is characterized by having the output process which outputs subject-copy image data including the pixel information restored at said restoration process.
[0017]
[Embodiment of the Invention] Hereafter, the gestalt of suitable operation of this invention is explained to a detail with reference to an accompanying drawing.
[0018] [Gestalt 1 of operation] drawing 1 is the block diagram showing the outline configuration of the digital-watermarking embedding equipment concerning the gestalt 1 of operation of this invention.
[0019] In drawing 1 , it embeds with the subject-copy image data x, and image data r is inputted into the input section 11. In the subject-copy image data x, are subject-copy image data which contain two or more pixels which consist of the locations and pixel values (brightness value) of the pixel, respectively here, and it sets in the gestalt 1 of this operation. One pixel data of subject-copy image data is data which consist of a red (R) component, a green (G) component, and a blue (B) component, and each color component is expressed by 256 gradation (8 bits). Moreover, embedding image data r is watermark image data which consists of a pixel location which shows the configuration of the image to embed.
[0020] Even if this embedding image data r is data of the contents which are meaningful with a user as shows drawing 9 etc., it may be any of the data of meaningless contents. For example, as data of meaningful contents, data which assert copyright information etc. can be considered like a logo mark. When embedding the information which shows a LOGO as shown in drawing 9 here, it is possible to constitute the data of a serial bit sequence in which this embedding image data r as shown in drawing 10 is shown by making a sign "1" correspond to a black pixel, and making a sign "0" correspond to a white pixel as information which shows a field. Moreover, the data case of meaningless contents can consider expressing for information which carries out the mask of the specific location of subject-copy image data.
[0021] The subject-copy image data x which were described above, and embedding image data r are set up in an initial state.

[0022] Next, in the change machine 12, when the pixel location of the pixel of the subject-copy image data x is compared with the configuration information on the watermark image contained in embedding image data r and they are in agreement, in the case of delivery and an inequality, the separation about the pixel and a spawn process are not performed for the pixel value whose location of the corresponds to an eliminator 13, but the pixel value of the subject-copy image data x is outputted to it as it is at the change machine 14.
[0023] The color component of at least one or more colors is separated from subject-copy image data among the color components of three colors which constitute the pixel value (all or part) of the pixel location where the subject-copy image

data x were specified from an eliminator 13, and the separated information is stored as key information k. Moreover, the remaining information that this key information k was separated (x1) It outputs to the change machine 14.
[0024] The color component information separated here has 256 gradation, i.e., the amount of information of 8 bits, in the gestalt 1 of this operation. Therefore, although 8 bits (key information k) of information to separate may be all and it may be less than 8 bits, it needs to be at least 1 bits or more. In addition, in order to perform watermark embedding processing of a visible mold effectively, without being dependent on the subject-copy image data x, it is desirable to separate 8 bits of all information. However, since it is outputted as key information k, it is necessary to control the separated information to lessen the amount of information of this key information k to separate to make this key information k small.
[0025] Furthermore, the number of the color components to separate can express the contents of the pixel location to which its attention is paid now by the two remaining colors, when it is one color. For example, even if it separates a red component, the remaining green components and a blue component can express the contents of the pixel location which is carrying out current view. However, in this case, since the red component is not contained, the tint of this pixel location will change. It can claim in visible that digital watermarking is clearly embedded to a user by change of this tint. Moreover, when the number of the color components to separate is three colors, the contents of the pixel location to which its attention is paid cannot be expressed. This may be an effective means for application by which he does not want to also tell the contents of the image to which its attention was paid. In addition, it can also perform to juxtaposition performing processing in the gestalt of this operation mentioned above one by one for every pixel.
[0026] By processing described above, it can space to subject-copy image data, and the deformation according to the configuration information on image data can be added. Since this deformation changes that pixel value a lot according to an eliminator 13 unlike above-mentioned invisible mold digital watermarking, it serves as a visible visible mold watermark. Thus, the image data (x1) separated with the eliminator 13 is inputted into the change machine 14. With this change vessel 14, when the pixel location of the pixel of the subject-copy image data x is compared with the configuration information on the watermark image contained in embedding image data r like the above-mentioned change machine 12 and they are in agreement, the image data (x1) inputted from an eliminator 13 is outputted to the output section 15, and, in the case of delivery and an inequality, it outputs the pixel value of the subject-copy image data x to the output section 15 as it is. Thus, the reconstititution of the image data where the watermark image was embedded is carried out, and the result is outputted to the output section 15. Furthermore, the key information k separated with the eliminator 13 is outputted to the output section 15. In this way, from the output section 15, embedding finishing image data x' and the key information k that the watermark image was embedded are outputted.
[0027] Below, the image data generated by processing of the gestalt 1 of this operation which was described above is called a visible mold digital-watermarking embedding finishing image.
[0028] This image can be reversibly restored by the decoding method shown in the gestalt 2 of the next operation, and if it is the information which has meanings, such as a copyright person's LOGO, as for the configuration of a watermark image, the effectiveness of different copyright information protection from a mere image scramble is realizable.
[0029] [Gestalt 2 of operation] drawing 2 is the block diagram showing the outline configuration of the digital-watermarking discharge equipment concerning the gestalt of operation of this invention.
[0030] In drawing 2 , visible mold digital-watermarking embedding finishing image x', embedding image data r, and the key information k are inputted from the input section 21. Here, visible mold digital-watermarking embedding finishing image x' is image data x' processed by the configuration explained with the gestalt 1 of the above-mentioned implementation, and embedding image data r is embedding image data r and the equal which were inputted in the gestalt 1 of the above-mentioned implementation. Furthermore, the key information k must be equal to the key information k outputted with the gestalt 1 of the above-mentioned implementation as explained. When such information, especially embedding image data r and the key information k are not inputted correctly, the processing in the gestalt 2 of this operation does not carry out normal termination. Normal termination is restoring the subject-copy image data x reversibly from visible mold digital-watermarking embedding finishing image x' here.
[0031] It is the watermark image configuration information (embedding image data) r which consists of a pixel location that the configuration of the image to embed is indicated to be visible mold digital-watermarking embedding finishing image x' which consists of two or more pixels which consist of the pixel location and pixel value with the gestalt 2 of this operation, respectively, and the embedding image data of the same serial bit sequence as what was used for embedding with the gestalt 1 of the above-mentioned implementation is set up in an initial state.
[0032] In the change machine 22 of drawing 2 , comparison processing with the pixel location of each pixel which constitutes digital-watermarking embedding finishing image x', and the pixel location of embedding image data r is performed, and when in agreement, the pixel positional information is not performed in the synthetic vessel 23, and, in the case of delivery and an inequality, synthetic processing about the pixel is not performed, but watermark embedding finishing image x' is changed, and it inputs into a vessel 24 as it is. In addition, since [a certain] the embedding image r in the gestalt 2 of this operation is the same as the embedding image r of the gestalt 1 of above-mentioned operation, watermark embedding finishing image x' which changes here and is inputted into a vessel 24 is equal to the subject-copy image data x in the gestalt 1 of operation as a result.
[0033] With the synthetic vessel 23, the pixel value (all or part) and the key information k at the time on the pixel location where subject-copy image data were specified are inputted, and the data of the key information k are compounded to this component paying attention to the component separated with the gestalt 1 of the above-mentioned implementation among the color components of three colors which constitute that pixel value. In addition, the method of the composition in this synthetic vessel 23 must be completely equivalent to the method of the separation in the eliminator 13 in the gestalt 1 of the above-mentioned implementation. That is, for example, when all the information on a red component (8 bits) is separated in the eliminator 13, it is necessary to compound all the information on a red component (8 bits) from the key information k in this synthetic vessel 23. In this way, the pixel value of an embedding image location becomes what was restored by the original subject-copy image data, and the image data outputted from the synthetic vessel 23 changes, and is outputted to a vessel 24. This change machine 24 makes the pixel value of the pixel location directed by embedding image data r the pixel value outputted from the synthetic vessel 23, and the pixel value of the other pixel location outputs the output of the change machine 22 as it is. In this way, removal image x" (equal to the subject-copy image data x of drawing 1) by which the digital-watermarking image was removed from embedding finishing image x' is inputted into the output section 25, and it is outputted to it as it is.
[0034] In addition, it can also perform performing processing in the gestalt 2 of this operation one by one for every pixel to juxtaposition. Visible mold digital-watermarking embedding finishing image x' generated by the gestalt 1 of the above-mentioned implementation by this is reversibly decoded by the subject-copy image data x.
[0035] [Gestalt 3 of operation] drawing 3 is the block diagram showing the outline configuration of the digital-watermarking

embedding equipment concerning the gestalt 3 of operation of this invention, and is enciphering and outputting the key information k outputted here. In addition, the same sign shows the part which is common in the configuration of drawing 1 concerning the gestalt 1 of the above-mentioned operation, and it omits those explanation.
[0036] The encryption machine 36 performs encryption processing to the outputted key information k. The key information k outputted by the gestalt 1 of the above-mentioned implementation here must serve as an input of the gestalt 2 of the above-mentioned implementation using a suitable transmission line. When the gestalt 1 of the above-mentioned implementation and the gestalt 2 of operation are applied to application it is possible only for the permitted user to perform digital-watermarking discharge to normal here, this key information k needs to be transmitted to insurance in said transmission line. Here, it means/or communicating, without being altered, without transmitting to insurance being intercepted by the 3rd person in a transmission line. In order to establish this safe transmission line, with the gestalt 3 of this operation, it transmits by enciphering the key information k.
[0037] Therefore, with this encryption vessel 36, suitable encryption processing is performed to the key information k generated by the eliminator 13, and enciphered key information k' is outputted.
[0038] It is possible to use DES (detailed to Ikeno, Oyama, the "present age code theory", and the Institute of Electronics, Information and Communication Engineers), FEAL, TDEA, RC2, RC4 and RC5, MISTY, the Caesar mold code, a BIJINERU code, the Beaufort code, a play fair code, a leech code, the Barnum code, etc. for encryption processing in this encryption machine 36 as a common key encryption system.
[0039] The same sign shows the part which drawing 4 is the schematic diagram of the digital-watermarking discharge equipment concerning the gestalt 4 of operation of this invention of which digital watermarking embedded with the digital-watermarking embedding equipment of drawing 3 is canceled, and is common in the configuration of above-mentioned drawing 2 , and it omits those explanation.
[0040] With the digital-watermarking discharge equipment of the gestalt 4 of this operation, the decoder 40 which decodes enciphered key information k' is formed. This decoder 40 performs decode processing to key information k' by which encryption processing was carried out. It is possible to realize discharge of digital watermarking embedded by the above-mentioned digital-watermarking embedding equipment like the configuration of above-mentioned drawing 2 using the key information k by which decode processing was carried out with this decoder 40.
[0041] [Gestalt 4 of operation] drawing 5 is the block diagram showing the configuration of the digital-watermarking embedding equipment concerning the gestalt 4 of operation of this invention, carries out the data compression of the key information k outputted in the gestalt 1 of above-mentioned operation with the data compression vessel 56, and is outputting it here. In addition, the same number shows the part which is common in the configuration of drawing 1 , and it omits those explanation.
[0042] The data compression machine 56 performs data compression processing to the outputted key information k. The key information k outputted by the gestalt 1 of the above-mentioned implementation must serve as an input of the gestalt 2 of the above-mentioned implementation using a suitable transmission line. here — the above — when a suitable transmission line is a channel represented by the Internet or are storages, such as CD-ROM, the smaller possible one of the amount of information of the key information k is desirable. Therefore, in order to make the amount of information of the key information k as small as possible, with the gestalt 4 of this operation, the data compression of the key information k is carried out, and it is transmitted. In this data compression machine 56, suitable data compression processing is performed to the key information k generated by the eliminator 13. The color information separated by this eliminator 13 has many redundant components, when image data, such as a LOGO, is spatially continuous. This is more remarkable when the subject-copy image data x are a common natural image like a photograph. Therefore, the effectiveness of a bigger data compression is expectable to the key information k.
[0043] The LZW method which uses a dictionary for this data compression processing as for example, a compression method, the Huffman coding based on statistical fluctuation, algebraic-sign-izing which improved Huffman coding are available. In addition, key information k" by which data compression processing was carried out with this data compression vessel 56 is used by the digital-watermarking discharge equipment mentioned later. For this reason, this compression method must be reversible processing.
[0044] Drawing 6 is the block diagram showing the configuration of the digital-watermarking discharge equipment concerning the gestalt 4 of operation of this invention, and cancels digital watermarking embedded with the digital-watermarking embedding equipment of above-mentioned drawing 5 . The configuration of the discharge equipment of the gestalt 4 of this operation is the same configuration except that the data defrosting machine 60 for thawing key information k" compressed as compared with the configuration of above-mentioned drawing 2 is formed. The same number shows the part which is common in drawing 2 , and it omits those explanation. This data defrosting machine 60 performs defrosting processing to key information k" by which data compression processing was carried out, and is outputting the thawed key information k.
[0045] Thus, it is possible to receive compressed key information k", to carry out defrosting processing, and to cancel digital watermarking embedded by digital-watermarking embedding equipment like the equipment of above-mentioned drawing 2 using the key information k on the origin of it thawed and obtained.
[0046] [Gestalt 5 of operation] drawing 7 is the block diagram showing the outline configuration of the digital-watermarking embedding equipment concerning the gestalt 5 of operation of this invention, the same number shows the part which is common in the configuration of the gestalt of the above-mentioned operation, and it omits those explanation.
[0047] With the gestalt 5 of this operation, it is alternatively made available combining the method which enciphers the key information k shown with the gestalt 3 of the above-mentioned operation, and the method which carries out data compression processing of the key information k stated with the gestalt 4 of said operation. In this case, it is more desirable to perform encryption processing from the property of the data of the key information k, after performing data compression processing.
[0048] The data with which this enciphered this to the ability to carry out data compression processing effectively mostly with a redundant component since the key information k had the property of the signal of general natural image data are because it does not have the property of the signal of general natural image data and it is expected that a redundant component decreases.
[0049] Furthermore, drawing 8 is the block diagram of the equipment of which digital watermarking embedded by the digital-watermarking embedding equipment concerning the gestalt 5 of operation of this invention shown in drawing 7 is canceled.
[0050] As shown in drawing 7 , the data compression of the key information k is carried out, and when enciphered, as shown in drawing 8 , the key information kx which the data compression was carried out and was enciphered needs to be thawed like the case of the equipment of drawing 2 after that, after decode processing is carried out with the data defrosting machine 60 and a decoder 40.
[0051] On the other hand, when data compression processing is performed after encryption processing of the key

information k is first carried out in the equipment shown by drawing 7 , decode processing needs to be carried out first and defrosting processing of the key information kx inputted into drawing 8 needs to be carried out after that.
[0052] This invention is not what is limited only to the approach of performing combining the equipment for realizing the gestalt of the above-mentioned implementation, an approach, and the approach explained with the gestalt of the above-mentioned implementation. To the computer in the above-mentioned system or equipment (CPU or MPU) The program code of the software for realizing the gestalt of the above-mentioned implementation is supplied, and also when the computer of the above-mentioned system or equipment operates the various above-mentioned devices according to this program code and it realizes the gestalt of the above-mentioned implementation, it is contained under the category of this invention.
[0053] Moreover, the program code of said software itself will realize the function of the gestalt of the above-mentioned implementation in this case, and the means for supplying that program code itself and its program code to a computer and the storage which specifically stored the above-mentioned program code are contained under the category of this invention.
[0054] As a storage which stores such a program code, a floppy (trademark) disk, a hard disk, an optical disk, a magneto-optic disk, CD-ROM, a magnetic tape, the memory card of a non-volatile, ROM, etc. can be used, for example.
[0055] Moreover, not only when the function of the gestalt of the above-mentioned implementation is realized, but when the above-mentioned computer controls various devices only according to the supplied program code, and the gestalt of the above-mentioned implementation is realized in collaboration with OS (operating system) to which the above-mentioned program code is working on a computer, or other application programs, this program code is contained under the category of this invention.
[0056] Furthermore, after this supplied program code is stored in the memory with which the functional expansion unit connected to the functional add-in board and the computer of a computer is equipped, a part or all of processing that CPU with which that functional add-in board and a functional storing unit are equipped based on directions of that program code is actual is performed, and also when the gestalt of the above-mentioned implementation is realized by that processing, it is contained under the category of this invention.
[0057] As explained above, according to the gestalt of this operation, it spaces with subject-copy image data, and the configuration information on an image is inputted, and the embedding finishing image which separated specific information from the pixel value of the pixel of the subject-copy image data contained in the watermark Image shown using the configuration information on the watermark image and which spaced and embedded the image is generated. At this time, the original subject-copy image can be restored by making separated specific information into key information using that key information.
[0058] Thereby, the high visible mold digital-watermarking embedding approach of security became possible.
[0059] Moreover, transmission of a visible mold digital-watermarking embedding image with more high security is attained by enciphering and transmitting the key information, decoding the key information by the receiving side which received it, and generating a subject-copy image.
[0060] Moreover, by compressing and transmitting the key information, thawing the key information by the receiving side which received it (expanding), and generating a subject-copy image, the amount of data to transmit is reduced and transmission of the high visible mold digital-watermarking embedding image of security is attained.
[0061] Furthermore, by performing both these encryption and a data compression, the amount of data to transmit is decreased more, and transmission of the high visible mold digital-watermarking embedding image of security is attained.
[0062]
[Effect of the Invention] As explained above, according to this invention, it can space with subject-copy image data, and the configuration information on an image can be inputted, and the image-processing approach and equipment which output the image data where the watermark image was embedded, and the information removed in order to embed the watermark image as key information can be offered.
[0063] Moreover, according to this invention, based on the image data where the watermark image was embedded, and the key information corresponding to the information removed in order to embed the watermark image, the image-processing approach and equipment which restore data for a subject-copy image can be offered.
[0064] Furthermore, since make into key information the image data where the watermark image was embedded, and information removed in order to embed that watermark image, and compress this key information, and it reaches [according to this invention space with subject-copy image data and input the configuration information on an image, and] further, or it enciphers and it outputs, the image amount of data is decreased more, and the high watermark embedding image of security can be formed.
[0065] Moreover, according to this invention, based on the image data where the watermark image was embedded, and the key information corresponding to the information removed in order to embed the watermark image which compressed, reached or was enciphered, data can be restored for a subject-copy image.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is a block diagram explaining the outline configuration of the digital-watermarking embedding equipment concerning the gestalt 1 of operation of this invention.
[Drawing 2] It is a block diagram explaining the outline configuration of the digital-watermarking discharge equipment concerning the gestalt 2 of operation of this invention.
[Drawing 3] It is a block diagram explaining the outline configuration of the digital-watermarking embedding equipment using encryption processing of key information concerning the gestalt 3 of operation of this invention.
[Drawing 4] It is a block diagram explaining the outline of digital-watermarking discharge equipment concerning the gestalt 3 of operation of this invention of receiving the enciphered key information and canceling electronic ******.
[Drawing 5] It is a block diagram explaining the outline of the digital-watermarking embedding equipment which compresses key information concerning the gestalt 4 of operation of this invention.
[Drawing 6] It is a block diagram explaining the outline configuration of the digital-watermarking discharge equipment at the time of using the compressed key information concerning the gestalt 4 of this operation.
[Drawing 7] It is a block diagram explaining the outline of the digital-watermarking embedding equipment at the time of using combining the encryption processing and data compression processing of key information concerning the gestalt 5 of operation of this invention.
[Drawing 8] It is a block diagram explaining the outline of digital-watermarking discharge equipment concerning the gestalt 5 of this operation of canceling digital watermarking based on the key information enciphered and compressed.
[Drawing 9] It is drawing explaining an example of the embedding image data concerning the gestalt of this operation.
[Drawing 10] It is drawing explaining the example of the field data made from the embedding image data shown in drawing 9 .

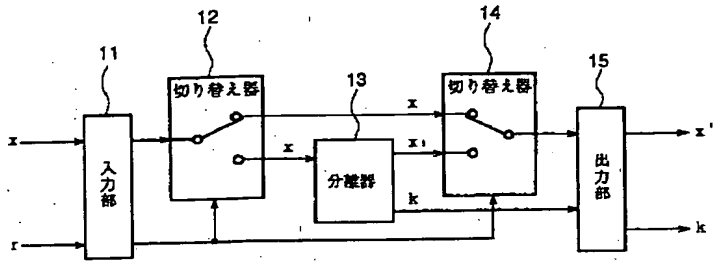
[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

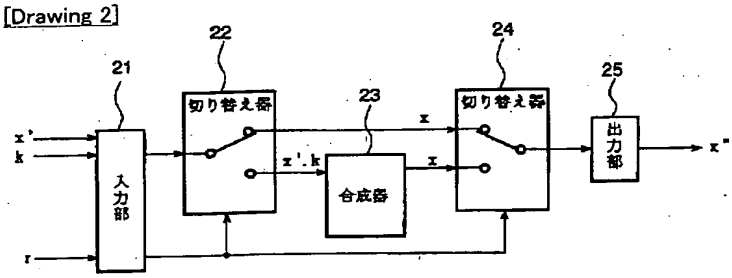
DRAWINGS

[Drawing 1]



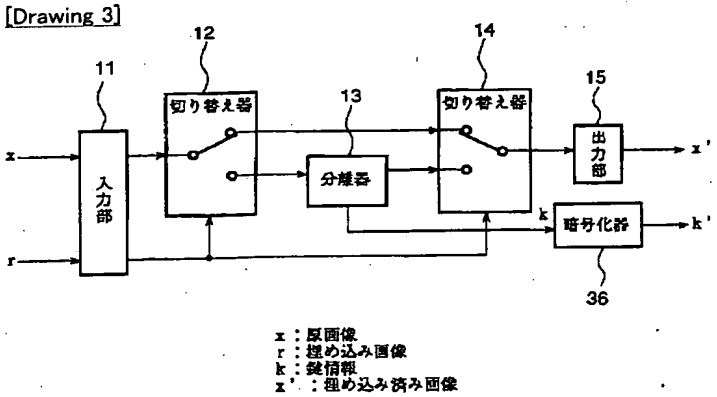
x：原画像
r：埋め込み画像
k：鍵情報
x'：埋め込み済み画像

[Drawing 2]



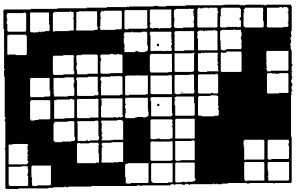
x'：埋め込み済み画像
x"：除去画像
r：埋め込み画像
k：鍵情報

[Drawing 3]



x：原画像
r：埋め込み画像
k：鍵情報
x'：埋め込み済み画像

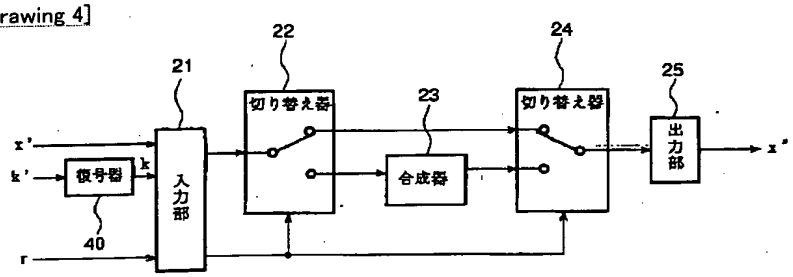
[Drawing 9]



[Drawing 10]

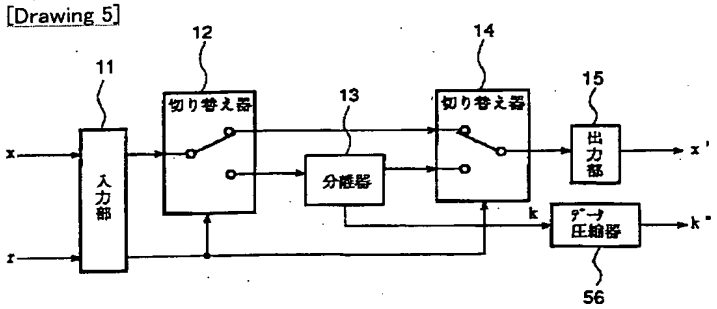
0	0	0	0	0	0	0	0	0	0	0	0
0	1	1	1	1	0	0	0	0	0	1	1
1	1	0	0	0	1	0	0	0	0	1	0
1	0	0	0	0	0	0	0	0	1	1	0
1	0	0	0	0	0	0	0	0	1	1	1
1	1	0	0	0	1	0	0	1	1	1	1
0	1	1	0	0	1	0	0	1	1	0	0
0	0	1	1	1	0	0	0	1	1	0	0

[Drawing 4]



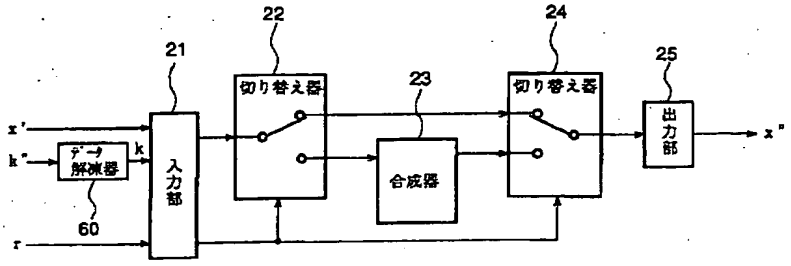
x' ：埋め込み済み画像
x" ：除去画像
r ：埋め込み画像
k ：鍵情報

[Drawing 5]



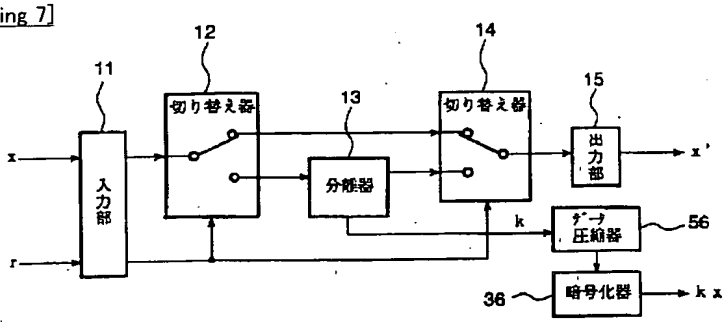
x ：原画像
r ：埋め込み画像
k ：鍵情報
x' ：埋め込み済み画像

[Drawing 6]



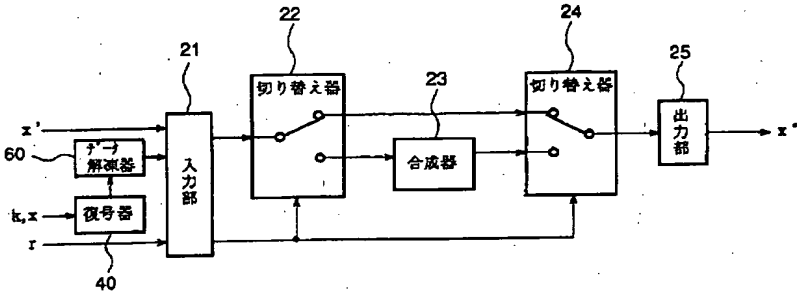
x' ：埋め込み済み画像
x" ：除去画像
r ：埋め込み画像
k ：鍵情報

[Drawing 7]



x：原画像
r：埋め込み画像
k：鍵情報
x'：埋め込み済み画像

[Drawing 8]



x'：埋め込み済み画像
x"：除去画像
r：埋め込み画像
k：鍵情報

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－24875
（P2001－24875A）
(43)公開日　平成13年１月26日(2001.1.26)

(51)Int.Cl.⁷		識別記号	FI		テーマコード（参考）
H04N	1/387		H04N	1/387	5B057
G06T	1/00		G09C	5/00	5C053
G09C	5/00		G06F	15/66	B 5C064
H04N	5/92		H04N	5/92	H 5C076
	7/167			7/167	Z 5J104

審査請求　未請求　請求項の数24　ＯＬ　（全 11 頁）

(21)出願番号　特願平11－193331

(22)出願日　平成11年７月７日(1999.7.7)

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目30番２号

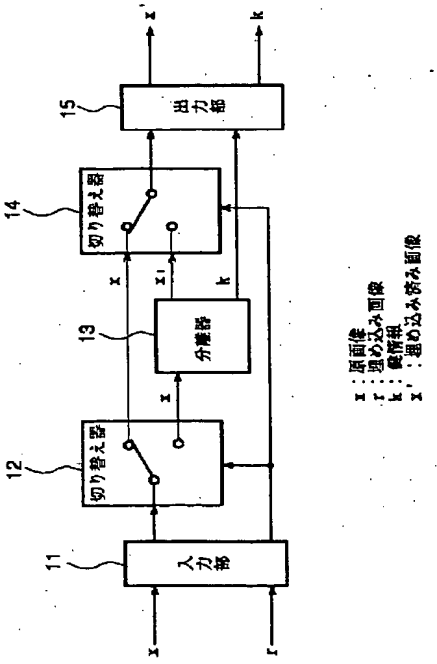
(72)発明者　林　淳一
東京都大田区下丸子３丁目30番２号　キヤノン株式会社内

(74)代理人　100076428
弁理士　大塚　康徳　（外２名）

最終頁に続く

(54)【発明の名称】　画像処理方法及び装置と記憶媒体

(57)【要約】
【課題】　原画像データと透かし画像の形状情報とを入力して、透かし画像が埋め込まれた画像データと、その透かし画像を埋め込むために除去された情報を鍵情報として出力し、その透かし画像が埋め込まれた画像データと、その透かし画像を埋め込むために除去された情報に対応する鍵情報とに基づいて、原画像をデータを復元する。
【解決手段】　原画像データｘと透かし画像の形状情報ｒを入力し、その形状情報ｒで指示される領域内に含まれる原画像データの画素情報を分離して変更し、その変更した画素情報に基づいて決定される鍵情報ｋを生成し、画素情報が変更された画像データｘ’と鍵情報ｋとを出力する。この画像データｘ’、透かし画像の形状情報ｒ及び鍵情報ｋを受取った側では、その形状情報ｒで指示される領域内に含まれる画像データの画素情報を鍵情報ｋに基づいて復元し、元の原画像データを生成する。



【特許請求の範囲】

【請求項1】 原画像データに透かし画像を埋め込む画像処理装置であって、
原画像データと前記透かし画像の形状情報を入力する入力手段と、
前記形状情報で指示される領域内に含まれる前記原画像データの画素情報を変更する変更手段と、
前記変更手段により変更された画素情報に基づいて決定される鍵情報を生成する鍵情報生成手段と、
前記変更手段により画素情報が変更された原画像データと前記鍵情報とを出力する出力手段と、を有することを特徴とする画像処理装置。

【請求項2】 前記変更手段は、
前記形状情報と前記原画像データの各画素位置とを比較し、前記形状情報に含まれる画素位置の画素値の所定の色成分の値を変更することを特徴とする請求項1に記載の画像処理装置。

【請求項3】 前記変更手段は、
前記形状情報と前記原画像データの各画素位置とを比較し、前記形状情報に含まれる画素位置の画素値の一部を変更することを特徴とする請求項1に記載の画像処理装置。

【請求項4】 前記鍵情報生成手段は、前記変更された画素情報と前記原画像データの対応する画素値との差分を基に前記鍵情報を生成することを特徴とする請求項1乃至3のいずれか1項に記載の画像処理装置。

【請求項5】 前記出力手段は、前記鍵情報を暗号化する暗号化手段を有することを特徴とする請求項1乃至4のいずれか1項に記載の画像処理装置。

【請求項6】 前記出力手段は、前記鍵情報を圧縮する圧縮手段を有することを特徴とする請求項1乃至5のいずれか1項に記載の画像処理装置。

【請求項7】 原画像データに透かし画像が埋め込まれた埋め込み画像データを入力して前記原画像データを復元する画像処理装置であって、
前記埋め込み画像データと、前記透かし画像の形状情報及び鍵情報を入力する入力手段と、
前記形状情報で指示される領域内に含まれる前記埋め込み画像データの画素情報を前記鍵情報に基づいて元の画素情報に復元する復元手段と、
前記復元手段により復元された画素情報を含む原画像データを出力する出力手段と、を有することを特徴とする画像処理装置。

【請求項8】 前記復元手段は、
前記形状情報と前記埋め込み画像データの各画素位置とを比較し、前記形状情報に含まれる画素位置の画素値の所定の色成分の値を前記鍵情報に従って変更することを特徴とする請求項7に記載の画像処理装置。

【請求項9】 前記復元手段は、
前記形状情報と前記埋め込み画像データの各画素位置とを比較し、前記形状情報に含まれる画素位置の画素値の一部を前記鍵情報に従って変更することを特徴とする請求項7に記載の画像処理装置。

【請求項10】 前記鍵情報は暗号化されており、当該鍵情報を復号する復号化手段を更に有することを特徴とする請求項7乃至9のいずれか1項に記載の画像処理装置。

【請求項11】 前記鍵情報はデータ圧縮されており、当該鍵情報を伸長する伸長手段を更に有することを特徴とする請求項7乃至10のいずれか1項に記載の画像処理装置。

【請求項12】 原画像データに透かし画像を埋め込む画像処理方法であって、
原画像データと前記透かし画像の形状情報を入力する入力工程と、
前記形状情報で指示される領域内に含まれる前記原画像データの画素情報を変更する変更工程と、
前記変更工程で変更された画素情報に基づいて決定される鍵情報を生成する鍵情報生成工程と、
前記変更工程で画素情報が変更された原画像データと前記鍵情報とを出力する出力工程と、を有することを特徴とする画像処理方法。

【請求項13】 前記変更工程では、
前記形状情報と前記原画像データの各画素位置とを比較し、前記形状情報に含まれる画素位置の画素値の所定の色成分の値を変更することを特徴とする請求項12に記載の画像処理方法。

【請求項14】 前記変更工程では、
前記形状情報と前記原画像データの各画素位置とを比較し、前記形状情報に含まれる画素位置の画素値の一部を変更することを特徴とする請求項12に記載の画像処理方法。

【請求項15】 前記鍵情報生成工程では、前記変更された画素情報と前記原画像データの対応する画素値との差分を基に前記鍵情報を生成することを特徴とする請求項12乃至14のいずれか1項に記載の画像処理方法。

【請求項16】 前記出力工程は、前記鍵情報を暗号化する暗号化工程を有することを特徴とする請求項12乃至15のいずれか1項に記載の画像処理方法。

【請求項17】 前記出力工程は、前記鍵情報を圧縮する圧縮工程を有することを特徴とする請求項12乃至16のいずれか1項に記載の画像処理方法。

【請求項18】 原画像データに透かし画像が埋め込まれた埋め込み画像データを入力して前記原画像データを復元する画像処理方法であって、
前記埋め込み画像データと、前記透かし画像の形状情報及び鍵情報を入力する入力工程と、
前記形状情報で指示される領域内に含まれる前記埋め込み画像データの画素情報を前記鍵情報に基づいて元の画素情報に復元する復元工程と、

前記復元工程で復元された画素情報を含む原画像データを出力する出力工程と、を有することを特徴とする画像処理方法。

【請求項１９】 前記復元工程では、

前記形状情報と前記埋め込み画像データの各画素位置とを比較し、前記形状情報に含まれる画素位置の画素値の所定の色成分の値を前記鍵情報に従って変更することを特徴とする請求項１８に記載の画像処理方法。

【請求項２０】 前記復元工程では、

前記形状情報と前記埋め込み画像データの各画素位置とを比較し、前記形状情報に含まれる画素位置の画素値の一部を前記鍵情報に従って変更することを特徴とする請求項１８に記載の画像処理方法。

【請求項２１】 前記鍵情報は暗号化されており、当該鍵情報を復号する復号化手段を更に有することを特徴とする請求項１８乃至２０のいずれか1項に記載の画像処理方法。

【請求項２２】 前記鍵情報はデータ圧縮されており、当該鍵情報を伸長する伸長工程を更に有することを特徴とする請求項１８乃至２１のいずれか1項に記載の画像処理方法。

【請求項２３】 原画像データに透かし画像を埋め込む画像処理方法を実行するプログラムを記憶する記憶媒体であって、

原画像データと前記透かし画像の形状情報を入力する入力工程モジュールと、

前記形状情報で指示される領域内に含まれる前記原画像データの画素情報を変更する変更工程モジュールと、

前記変更工程で変更された画素情報に基づいて決定される鍵情報を生成する鍵情報生成工程モジュールと、

前記変更工程で画素情報が変更された原画像データと前記鍵情報とを出力する出力工程モジュールと、を有することを特徴とする記憶媒体。

【請求項２４】 原画像データに透かし画像が埋め込まれた埋め込み画像データを入力して前記原画像データを復元する画像処理方法を実行するプログラムを記憶した記憶媒体であって、

前記埋め込み画像データと、前記透かし画像の形状情報及び鍵情報を入力する入力工程モジュールと、

前記形状情報で指示される領域内に含まれる前記埋め込み画像データの画素情報を前記鍵情報に基づいて元の画素情報に復元する復元工程モジュールと、

前記復元工程で復元された画素情報を含む原画像データを出力する出力工程モジュールと、を有することを特徴とする記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、原画像データに電子透かしを埋め込んだ画像データを生成し、及び或はその画像データから電子透かし部分を除去して原画像データを生成する画像処理方法及び装置と記憶媒体に関するものである。

【０００２】

【従来の技術】画像をデジタル信号として扱うデジタル画像は、従来のアナログ信号で表現されるアナログ画像と比較して、コンピュータなどによって簡単にコピーでき、しかもその様な複写を行っても画質が劣化することがない等の特徴があり、しかも通信回線を通して遠隔地に画質の劣化無く伝送できるといった利点がある。しかし、このような特徴により、デジタル画像は第三者により容易に不正コピーされ再配布されるという問題がある。これを防ぐための方法の一つとに、電子透かしと呼ばれる手法がある。

【０００３】この電子透かしには大きく分類して、著作権情報、ユーザ情報等の透かし情報を目に見えない形で画像に埋め込む不可視型と、その著作権を保有する会社のロゴ等の透かし画像を目に見える形で、その画像上に形成する可視型とがある。前者の不可視型の電子透かしでは、その埋め込み画像を一見しただけでは、透かし情報が埋め込まれていることが認識できない。従って、透かし情報の削除は行われにくいものの、その画像の不正コピー、不正編集は可視型の場合に比べて行われ易い。但し、例えデジタル画像データが不正にコピー又は編集された場合でも、そのデジタル画像データ中には透かし情報が残っているので、透かし情報として埋め込まれたユーザＩＤ等により、不正なコピー等を行ったユーザを特定することができる。

【０００４】このような不可視型の電子透かしの代表的なものとして、入力画像に対し高速フーリエ変換、離散コサイン変換、ウェーブレット変換等の周波数変換を行い、周波数領域に透かし情報を加えた後、逆周波数変換を行うことにより、電子透かしの埋め込みを行う手法が挙げられる。このうち、高速フーリエ変換による手法では、入力画像はＰＮ系列を加えられて拡散された後、ブロックに分割され、各ブロック毎にフーリエ変換が施され、１ブロックに1ビットの透かし情報が埋め込まれる。こうして透かし情報が埋め込まれたブロックに逆フーリエ変換が施され、再び最初と同じＰＮ系列が加えられて合成画像となる。この技術は例えば、大西、岡、松井等による、“ＰＮ系列による画像への透かし署名法”（１９９７年、暗号と情報セキュリティシンポジウム講演論文集、SCIS97-26B）に詳しい。また離散コサイン変換による手法は、ブロックに分割し、ブロック毎に離散コサイン変換をする。１ブロックに1ビットの情報を埋め込んだ後、逆変換をして合成画像を生成する。これは、例えば、中村、小川、高嶋等による“ディジタル画像の著作権保護のための周波数領域における電子透かし方式”（１９９７年、暗号と情報セキュリティシンポジウム講演論文集、SCIS97-26A）に詳しい。更にウェーブレット変換による手法は、入力画像をブロック分割する

必要のない手法で、これは石塚、酒井、櫻井等による“ウェーブレット変換を用いた電子すかし技術の安全性と信頼性に関する実験的考察”（１９９７年、暗号と情報セキュリティシンポジウム講演論文集、SCIS97-26D）に詳しい。また、画素の色相、明度等に演算を施して電子透かしを埋め込む手法（Digimarc社、米国特許5,636,292等）もある。

【０００５】一方、可視型の電子透かしでは、透かし情報はデジタル画像上に目で見える形で書き込まれているので、そのままでは利用し辛く、不正コピー、不正編集を思い留まらせる効果がある。このような可視型電子透かしは、正しい利用者だけが完全に透かし情報を取り除くことが可能であるように構成されている場合もある。その具体例として、その画像データの正規でない利用者に対しては、可視型の透かしが埋め込まれた画像を配布し、正規の利用者に対しては、可視型の透かしが埋め込まれていない画像を配布する場合が考えられる。

【０００６】これを実現するための一つの方法として、従来はロゴなどの画像の画素値を原画像の画素値と置き換えることにより、著作権情報を原画像データに貼り込み、正規でない利用者に対してはロゴ等を貼り込んだ画像データを配布し、正規の利用者に対しては原画像データをそのまま配布する方式が用いられてきた。しかし、可視型の電子透かしを埋め込んだ画像データの部分の内容は、ロゴなどの画像の内容に置き換えられているために、利用者はこの部分に対応する原画像データの内容を知ることができない。更に、このような電子透かしを除去するためには、原画像データの全てを送信する必要があるが、一般に原画像データは非常に大きなデータであるため、これを送信するには多くの時間が必要とされた。

【０００７】またこれとは他に、特開平8-241403号公報で提案されている方式もある。これは、原画像データの輝度値を線形変換することによって、色度を保存して可視型の電子透かしを埋め込む方式である。この方式では、可視型の電子透かしが埋め込まれた領域の原画像データの内容を使用者が知ることが可能であったが、可視型の電子透かしを解除する方法は明確にされていない。

【０００８】

【発明が解決しようとする課題】以上説明したように従来は、原画像データに可視型の電子透かしを埋め込み、その電子透かしが埋め込まれた画像データから電子透かし部分を解除する方法については提案されていない。このため、正規の利用者に対して可視型の電子透かしを解除した原画像データを提供するためには、その利用者に対して、その原画像のデータの全てを送信する必要があった。このような全原画像データの送信は多くの時間を要し、伝送コストの点でも問題となっていた。

【０００９】本発明は上記従来例に鑑みてなされたもので、原画像データと透かし画像の形状情報とを入力して、透かし画像が埋め込まれた画像データと、その透かし画像を埋め込むために除去された情報を鍵情報として出力する画像処理方法及び装置を提供することを目的とする。

【００１０】また本発明の目的は、透かし画像が埋め込まれた画像データと、その透かし画像を埋め込むために除去された情報に対応する鍵情報とに基づいて、原画像をデータを復元する画像処理方法及び装置を提供することにある。

【００１１】更に、本発明の目的は、原画像データと透かし画像の形状情報とを入力して、透かし画像が埋め込まれた画像データと、その透かし画像を埋め込むために除去された情報を鍵情報とし、更にこの鍵情報を圧縮、及び或は暗号化して出力する画像処理方法及び装置を提供することを目的とする。

【００１２】また本発明の目的は、透かし画像が埋め込まれた画像データと、その透かし画像を埋め込むために除去された情報に対応する、圧縮、及び或は暗号化された鍵情報とに基づいて、原画像をデータを復元する画像処理方法及び装置を提供することにある。

【００１３】

【課題を解決するための手段】上記目的を達成するために本発明の画像処理装置は以下のような構成を備える。即ち、原画像データに透かし画像を埋め込む画像処理装置であって、原画像データと前記透かし画像の形状情報を入力する入力手段と、前記形状情報で指示される領域内に含まれる前記原画像データの画素情報を変更する変更手段と、前記変更手段により変更された画素情報に基づいて決定される鍵情報を生成する鍵情報生成手段と、前記変更手段により画素情報が変更された原画像データと前記鍵情報とを出力する出力手段と、を有することを特徴とする。

【００１４】上記目的を達成するために本発明の画像処理装置は以下のような構成を備える。即ち、原画像データに透かし画像が埋め込まれた埋め込み画像データを入力して前記原画像データを復元する画像処理装置であって、前記埋め込み画像データと、前記透かし画像の形状情報及び鍵情報を入力する入力手段と、前記形状情報で指示される領域内に含まれる前記埋め込み画像データの画素情報を前記鍵情報に基づいて元の画素情報に復元する復元手段と、前記復元手段により復元された画素情報を含む原画像データを出力する出力手段とを有することを特徴とする。

【００１５】上記目的を達成するために本発明の画像処理方法は以下のような工程を備える。即ち、原画像データに透かし画像を埋め込む画像処理方法であって、原画像データと前記透かし画像の形状情報を入力する入力工程と、前記形状情報で指示される領域内に含まれる前記原画像データの画素情報を変更する変更工程と、前記変

更工程で変更された画素情報に基づいて決定される鍵情報を生成する鍵情報生成工程と、前記変更工程で画素情報が変更された原画像データと前記鍵情報とを出力する出力工程とを有することを特徴とする。

【００１６】上記目的を達成するために本発明の画像処理方法は以下のような工程を備える。即ち、原画像データに透かし画像が埋め込まれた埋め込み画像データを入力して前記原画像データを復元する画像処理方法であって、前記埋め込み画像データと、前記透かし画像の形状情報及び鍵情報を入力する入力工程と、前記形状情報で指示される領域内に含まれる前記埋め込み画像データの画素情報を前記鍵情報に基づいて元の画素情報に復元する復元工程と、前記復元工程で復元された画素情報を含む原画像データを出力する出力工程とを有することを特徴とする。

【００１７】

【発明の実施の形態】以下、添付図面を参照して本発明の好適な実施の形態を詳細に説明する。

【００１８】[実施の形態1]図1は、本発明の実施の形態1に係る電子透かし埋め込み装置の概略構成を示すブロック図である。

【００１９】図1において、原画像データｘと埋め込み画像データｒが入力部１１に入力される。ここで原画像データｘとは、それぞれが、その画素の位置と画素値（輝度値）とで構成される複数の画素を含む原画像データであり、本実施の形態1においては、原画像データの１つの画素データは、赤色（Ｒ）成分、緑色（Ｇ）成分、青色（Ｂ）成分で構成されるデータであり、それぞれの色成分は２５６階調（８ビット）で表現される。また、埋め込み画像データｒは、埋め込む画像の形状を示す画素位置からなる透かし画像データである。

【００２０】この埋め込み画像データｒは、例えば図9に示すような、利用者などによって意味のある内容のデータであっても、意味の無い内容のデータのいずれであっても良い。例えば、意味のある内容のデータとしては、ロゴマークなどのように、著作権情報などを主張するようなデータが考えられる。ここで図9に示すようなロゴを示す情報を埋め込む場合には、領域を示す情報として、黒色画素には符号“１”を対応させ、白色画素には符号“０”を対応させることによって、図１０に示すような、この埋め込み画像データｒを示すシリアルビット系列のデータを構成することが可能である。また意味の無い内容のデータ場合は、原画像データの特定位置をマスクするような情報で表現することが考えられる。

【００２１】以上述べたような原画像データｘ、及び埋め込み画像データｒが、初期状態において設定される。

【００２２】次に、切替え器１２において、原画像データｘの画素の画素位置と、埋め込み画像データｒに含まれる透かし画像の形状情報とを比較し、それらが一致した場合は、分離器１３に、その位置が一致する画素値を送り、不一致の場合は、その画素についての分離、切替え処理を行わず、原画像データｘの画素値をそのまま切替え器１４に出力する。

【００２３】分離器１３では、原画像データｘの指定された画素位置の画素値（全部又は一部）を構成する３色の色成分のうち、少なくとも１色以上の色成分を原画像データから分離し、その分離した情報を鍵情報kとして格納する。またこの鍵情報kが分離された残りの情報(x1)を、切替え器１４に出力する。

【００２４】ここで分離される色成分情報は、本実施の形態1においては２５６階調、即ち8ビットの情報量をもつ。よって、分離する情報（鍵情報k）は、８ビット全てであってもよいし、８ビット未満であってもよいが、少なくとも１ビット以上である必要がある。なお、原画像データｘに依存せずに、効果的に可視型の透かし埋め込み処理を行うためには、８ビット全ての情報を分離することが望ましい。しかしながら、分離した情報は鍵情報kとして出力されるため、この鍵情報kを小さくしたい場合には、この分離する鍵情報kの情報量を少なくするように制御する必要がある。

【００２５】更に、分離する色成分の数は、１色である場合は、残りの2色によって、現在着目している画素位置の内容を表現することが可能である。例えば、赤色成分を分離したとしても、残りの緑色成分、青色成分によって、現在着目している画素位置の内容が表現可能である。但し、この場合は、赤色成分が含まれていないために、この画素位置の色合いが変化してしまう。この色合いの変化によって、利用者に対して明示的に電子透かしが埋め込まれていることを可視的に主張することができる。また、分離する色成分の数が3色である場合には、その着目している画素位置の内容を表現することができない。これは着目した画像の内容も知らせたくないようなアプリケーションにとって有効な手段であるかもしれない。尚、上述した本実施の形態における処理は、各画素毎に順次行うことも、並列に行うこともできる。

【００２６】以上述べた処理によって、原画像データに対して透かし画像データの形状情報に応じた変形を加えることができる。この変形は上述の不可視型電子透かしと異なり、その画素値を分離器１３に応じて大きく変えるので、目に見える可視型透かしとなる。このようにして分離器１３で分離された画像データ(x1)は切替え器１４に入力される。この切替え器１４では、前述の切替え器１２と同様に、原画像データｘの画素の画素位置と、埋め込み画像データｒに含まれる透かし画像の形状情報とを比較し、それらが一致した場合は、分離器１３から入力される画像データ(x1)を出力部１５に送り、不一致の場合は、原画像データｘの画素値をそのまま出力部１５に出力する。このようにして、透かし画像が埋め込まれた画像データを再形成し、その結果が出力部１５に出力される。更に、分離器１３で分離された鍵情報kも出

力部15に出力される。こうして出力部15から、透かし画像が埋め込まれた埋め込み済み画像データx'と鍵情報kとが出力される。

【0027】以上述べたような本実施の形態1の処理によって生成される画像データを、以下では可視型電子透かし埋め込み済み画像と呼ぶ。

【0028】この画像は次の実施の形態2に示す復号法によって可逆的に復元可能であり、透かし画像の形状が著作権者のロゴ等、意味のある情報であれば単なる画像スクランブルと異なる著作権情報保護の効果を実現することが出来る。

【0029】[実施の形態2]図2は、本発明の実施の形態に係る電子透かし解除装置の概略構成を示すブロック図である。

【0030】図2において、可視型電子透かし埋め込み済み画像x'と、埋め込み画像データr、及び鍵情報kが入力部21より入力される。ここで、可視型電子透かし埋め込み済み画像x'とは、上記実施の形態1で説明した構成によって処理された画像データx'であり、埋め込み画像データrは、上記実施の形態1において入力された埋め込み画像データrと等しいものである。更に鍵情報kは、上記実施の形態1で説明したようにして出力された鍵情報kに等しくなければならない。これらの情報、特に埋め込み画像データrと鍵情報kが正しく入力されない場合には、本実施の形態2における処理は正常な終了をしない。ここで正常な終了とは、可視型電子透かし埋め込み済み画像x'から可逆的に原画像データxを復元することである。

【0031】本実施の形態2では、それぞれが、その画素位置と画素値で構成される複数の画素からなる可視型電子透かし埋め込み済み画像x'と、埋め込む画像の形状を示す画素位置からなる透かし画像形状情報(埋め込み画像データ)rであって、上記実施の形態1で埋め込みに用いたものと同じシリアルビット系列の埋め込み画像データを初期状態において設定する。

【0032】図2の切替え器22において、電子透かし埋め込み済み画像x'を構成する各画素の画素位置と、埋め込み画像データrの画素位置との比較処理を行い、一致した場合は、合成器23にその画素位置情報を送り、不一致の場合は、その画素についての合成処理を行わず、透かし埋め込み済み画像x'を切替え器24にそのまま入力する。なお、ここで切替え器24に入力される透かし埋め込み済み画像x'は、この実施の形態2における埋め込み画像rが上述の実施の形態1の埋め込み画像rと同じであるあるため、結果的に、実施の形態1における原画像データxに等しくなっている。

【0033】合成器23では、原画像データの指定された画素位置の画素値(全部又は一部)と、その時の鍵情報kを入力し、その画素値を構成する3色の色成分のうち、上記実施の形態1で分離された成分に着目し、この成分に対して鍵情報kのデータを合成する。尚、この合成器23における合成の方式は、上記実施の形態1における分離器13における分離の方式に完全に対応していなくてはならない。即ち例えば、分離器13において赤色成分の全ての情報(8ビット)が分離されていた場合には、この合成器23において赤色成分の全ての情報(8ビット)を鍵情報kから合成する必要がある。こうして合成器23から出力される画像データは、埋め込み画像位置の画素値が元の原画像データに修復されたものとなって切替え器24に出力される。この切替え器24は、埋め込み画像データrで指示された画素位置の画素値を合成器23から出力された画素値とし、それ以外の画素位置の画素値は切替え器22の出力をそのまま出力する。こうして出力部25には、埋め込み済み画像x'から電子透かし画像が除去された除去画像x"(図1の原画像データxに等しい)が入力され、そのまま出力される。

【0034】尚、本実施の形態2における処理は、各画素毎に順次行うことも、或は並列に行うこともできる。これによって、上記実施の形態1によって生成された可視型電子透かし埋め込み済み画像x'は可逆的に原画像データxに復号される。

【0035】[実施の形態3]図3は、本発明の実施の形態3に係る電子透かし埋め込み装置の概略構成を示すブロック図で、ここでは出力される鍵情報kを暗号化して出力している。尚、前述の実施の形態1に係る図1の構成と共通する部分は同じ符号で示し、それらの説明を省略する。

【0036】暗号化器36は、出力された鍵情報kに対して暗号化処理を行うものである。ここで上記実施の形態1によって出力された鍵情報kは、適当な伝送路を用いて上記実施の形態2の入力とならなければならない。ここで、上記実施の形態1及び実施の形態2が、許可された利用者だけが正常に電子透かし解除を実行することが可能であるようなアプリケーションに適用される場合には、この鍵情報kは前記伝送路において安全に伝送される必要がある。ここで、安全に伝送するとは、伝送路において、第3者によって盗聴されることなく、且つ/或いは改竄されることなく通信されることを意味している。この安全な伝送路を確立するために、本実施の形態3では鍵情報kを暗号化することにより伝送する。

【0037】従って、この暗号化器36では、分離器13によって生成された鍵情報kに対して適当な暗号化処理を行い、暗号化された鍵情報k'を出力している。

【0038】この暗号化器36における暗号化処理には、例えば、共通鍵暗号方式としてDES(池野、小山、"現代暗号理論"、電子情報通信学会に詳しい)、FEAL, TDEA, RC2, RC4, RC5, MISTY, シーザー型暗号、ビジネル暗号、ビューフォート暗号、プレイフェア暗号、ヒル暗号、バーナム暗号等を

用いることが可能である。

【００３９】図4は、図3の電子透かし埋め込み装置によって埋め込んだ電子透かしを解除する、本発明の実施の形態4に係る電子透かし解除装置の概略図で、前述の図2の構成と共通する部分は同じ符号で示し、それらの説明を省略する。

【００４０】この実施の形態4の電子透かし解除装置では、暗号化された鍵情報k'を復号する復号器４０を設けている。この復号器４０は、暗号化処理された鍵情報k'に対して復号処理を行う。この復号器４０により復号処理された鍵情報kを用いて、上記電子透かし埋め込み装置によって、前述の図2の構成と同様に、埋め込まれた電子透かしの解除を実現することが可能である。

【００４１】[実施の形態4]図5は、本発明の実施の形態4に係る電子透かし埋め込み装置の構成を示すブロック図で、ここでは上述の実施の形態1において出力された鍵情報kをデータ圧縮器５６によりデータ圧縮して出力している。尚、図1の構成と共通する部分は同じ番号で示し、それらの説明を省略する。

【００４２】データ圧縮器５６は、出力された鍵情報kに対してデータ圧縮処理を行うものである。上記実施の形態1によって出力された鍵情報kは、適当な伝送路を用いて上記実施の形態2の入力とならなければならない。ここで、上記適当な伝送路がインターネットに代表される通信路であったり、或いはCD-ROMなどの記憶媒体である場合には、鍵情報kの情報量はできる限り小さいほうが望ましい。よって、鍵情報kの情報量をできる限り小さくするために、本実施の形態4では、鍵情報kをデータ圧縮して伝送している。このデータ圧縮器５６においては、分離器１３によって生成された鍵情報kに対して適当なデータ圧縮処理を行う。この分離器１３によって分離された色情報は、ロゴ等の画像データが空間的に連続的である時には、冗長な成分を多く持つ。これは原画像データxが写真のような一般的な自然画像である場合には、より顕著である。よって、鍵情報kに対して、より大きなデータ圧縮の効果が期待できる。

【００４３】このデータ圧縮処理には、例えば圧縮方式としては、辞書を用いるＬＺＷ方式や、統計的変動に基づくハフマン符号化や、ハフマン符号化を改良した算術符号化などが利用可能である。尚、このデータ圧縮器５６によってデータ圧縮処理された鍵情報k"は、後述する電子透かし解除装置によって利用される。このために、この圧縮方式は可逆的な処理でなければならない。

【００４４】図6は、本発明の実施の形態4に係る電子透かし解除装置の構成を示すブロック図で、前述の図5の電子透かし埋め込み装置によって埋め込んだ電子透かしを解除する。この実施の形態4の解除装置の構成は、前述の図2の構成と比較すると、圧縮された鍵情報k"を解凍するためのデータ解凍器６０が設けられている以外は同じ構成である。図2と共通する部分は同じ番号で示し、それらの説明を省略する。このデータ解凍器６０は、データ圧縮処理された鍵情報k"に対して解凍処理を行い、解凍した鍵情報kを出力している。

【００４５】このようにして、圧縮された鍵情報k"を受信して解凍処理し、その解凍して得られた元の鍵情報kを用いて、前述の図2の装置と同様にして、電子透かし埋め込み装置によって埋め込まれた電子透かしを解除することが可能である。

【００４６】[実施の形態5]図7は、本発明の実施の形態5に係る電子透かし埋め込み装置の概略構成を示すブロック図で、前述の実施の形態の構成と共通する部分は同じ番号で示し、それらの説明を省略する。

【００４７】この実施の形態5では、前述の実施の形態３で示した鍵情報kを暗号化する方式と、前記実施の形態4で述べた鍵情報kをデータ圧縮処理する方式とを組み合わせて選択的に利用可能にしている。この場合、鍵情報kのデータの性質から、データ圧縮処理を行った後に暗号化処理を行うほうが望ましい。

【００４８】これは鍵情報kは、一般的な自然画像データの信号の性質を持つため、冗長な成分を多く持ちデータ圧縮処理を効果的に実施することができるのに対して、これを暗号化したデータは、一般的な自然画像データの信号の性質を持たない、且つ冗長な成分が少なくなることが予想されるためである。

【００４９】更に図8は、本発明の実施の形態5に係る、図7に示す電子透かし埋め込み装置により埋め込まれた電子透かしを解除する装置のブロック図である。

【００５０】図7に示すように、鍵情報kがデータ圧縮され、その後、暗号化されている場合には、図8に示すように、そのデータ圧縮され暗号化された鍵情報k xは、データ解凍器６０及び復号器４０で復号処理された後、図2の装置の場合と同様にして、解凍される必要がある。

【００５１】一方、図7で示した装置において、鍵情報kが最初に暗号化処理された後にデータ圧縮処理が行われている場合には、図8に入力された鍵情報k xは、最初に復号処理され、その後、解凍処理される必要がある。

【００５２】本発明は、上記実施の形態を実現するための装置及び方法、及び上記実施の形態で説明した方法を組み合わせて行う方法のみに限定されるものではなく、上記システム又は装置内のコンピュータ（ＣＰＵあるいはMPU）に、上記実施の形態を実現するためのソフトウエアのプログラムコードを供給し、このプログラムコードに従って上記システム或は装置のコンピュータが上記各種デバイスを動作させることにより上記実施の形態を実現する場合も本発明の範疇に含まれる。

【００５３】またこの場合、前記ソフトウエアのプログラムコード自体が上記実施の形態の機能を実現することになり、そのプログラムコード自体、及びそのプログラ

ムコードをコンピュータに供給するための手段、具体的には上記プログラムコードを格納した記憶媒体は本発明の範疇に含まれる。

【００５４】この様なプログラムコードを格納する記憶媒体としては、例えばフロッピー（登録商標）ディスク，ハードディスク，光ディスク，光磁気ディスク，ＣＤ-ＲＯＭ，磁気テープ，不揮発性のメモリカード，ＲＯＭ等を用いることができる。

【００５５】また、上記コンピュータが、供給されたプログラムコードのみに従って各種デバイスを制御することにより、上記実施の形態の機能が実現される場合だけではなく、上記プログラムコードがコンピュータ上で稼働しているＯＳ（オペレーティングシステム）、或は他のアプリケーション・プログラム等と共同して上記実施の形態が実現される場合にもかかるプログラムコードは本発明の範疇に含まれる。

【００５６】更に、この供給されたプログラムコードが、コンピュータの機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに格納された後、そのプログラムコードの指示に基づいてその機能拡張ボードや機能格納ユニットに備わるＣＰＵ等が実際の処理の一部または全部を行い、その処理によって上記実施の形態が実現される場合も本発明の範疇に含まれる。

【００５７】以上説明したように本実施の形態によれば、原画像データと透かし画像の形状情報を入力し、その透かし画像の形状情報によって示される透かし画像に含まれる原画像データの画素の画素値から特定の情報を分離した透かし画像を埋め込んだ埋め込み済み画像を生成する。このとき、分離した特定の情報を鍵情報とすることにより、その鍵情報を用いて、元の原画像を復元することができる。

【００５８】これにより、セキュリティが高い可視型電子透かし埋め込み方法が可能となった。

【００５９】また、その鍵情報を暗号化して伝送し、それを受信した受信側でその鍵情報を復号して原画像を生成することにより、よりセキュリティの高い可視型電子透かし埋め込み画像の送信が可能になる。

【００６０】また、その鍵情報を圧縮して伝送し、それを受信した受信側でその鍵情報を解凍（伸長）して原画像を生成することにより、伝送するデータ量を減らし、かつセキュリティの高い可視型電子透かし埋め込み画像の送信が可能になる。

【００６１】また更に、これら暗号化及びデータ圧縮の両方を行うことにより、伝送するデータ量をより減少させ、かつセキュリティの高い可視型電子透かし埋め込み画像の送信が可能になる。

【００６２】

【発明の効果】以上説明したように本発明によれば、原画像データと透かし画像の形状情報とを入力して、透かし画像が埋め込まれた画像データと、その透かし画像を埋め込むために除去された情報を鍵情報として出力する画像処理方法及び装置を提供することができる。

【００６３】また本発明によれば、透かし画像が埋め込まれた画像データと、その透かし画像を埋め込むために除去された情報に対応する鍵情報とに基づいて、原画像をデータを復元する画像処理方法及び装置を提供することができる。

【００６４】更に、本発明によれば、原画像データと透かし画像の形状情報とを入力して、透かし画像が埋め込まれた画像データと、その透かし画像を埋め込むために除去された情報を鍵情報とし、更にこの鍵情報を圧縮、及び或は暗号化して出力するので、画像データ量をより減少させ、かつセキュリティの高い透かし埋め込み画像を形成できる。

【００６５】また本発明によれば、透かし画像が埋め込まれた画像データと、その透かし画像を埋め込むために除去された情報に対応する、圧縮、及び或は暗号化された鍵情報とに基づいて、原画像をデータを復元することができる。

【図面の簡単な説明】

【図１】本発明の実施の形態1に係る電子透かし埋め込み装置の概略構成を説明するブロック図である。

【図２】本発明の実施の形態2に係る電子透かし解除装置の概略構成を説明するブロック図である。

【図３】本発明の実施の形態3に係る、鍵情報の暗号化処理を用いた電子透かし埋め込み装置の概略構成を説明するブロック図である。

【図４】本発明の実施の形態3に係る、暗号化された鍵情報を受信して電子つ可視を解除する電子透かし解除装置の概略を説明するブロック図である。

【図５】本発明の実施の形態4に係る、鍵情報を圧縮する電子透かし埋め込み装置の概略を説明するブロック図である。

【図６】本実施の形態4に係る、圧縮された鍵情報を用いた場合の電子透かし解除装置の概略構成を説明するブロック図である。

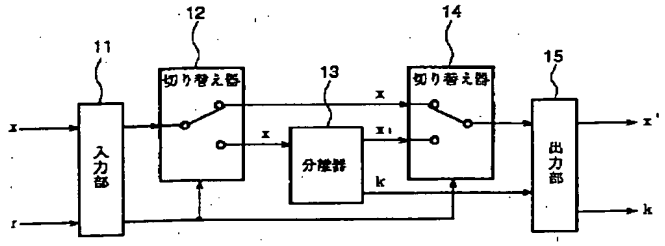
【図７】本発明の実施の形態5に係る、鍵情報の暗号化処理とデータ圧縮処理を組み合わせて用いた場合の電子透かし埋め込み装置の概略を説明するブロック図である。

【図８】本実施の形態5に係る、暗号化され圧縮された鍵情報を基に電子透かしを解除する電子透かし解除装置の概略を説明するブロック図である。

【図９】本実施の形態に係る埋め込み画像データの一例を説明する図である。

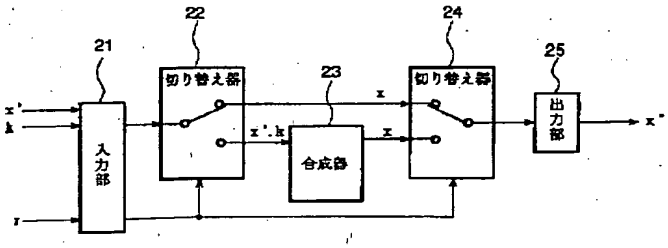
【図１０】図9に示す埋め込み画像データから作られた領域データの例を説明する図である。

【 図1 】



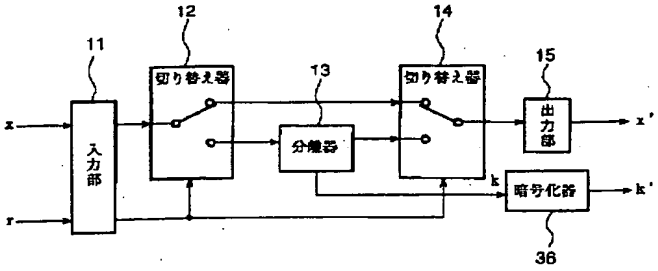
x：原画像
r：埋め込み画像
k：鍵情報
x'：埋め込み済み画像

【 図2 】



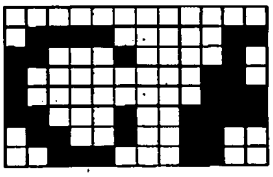
x'：埋め込み済み画像
x"：除去画像
r：埋め込み画像
k：鍵情報

【 図3 】



x：原画像
r：埋め込み画像
k：鍵情報
x'：埋め込み済み画像

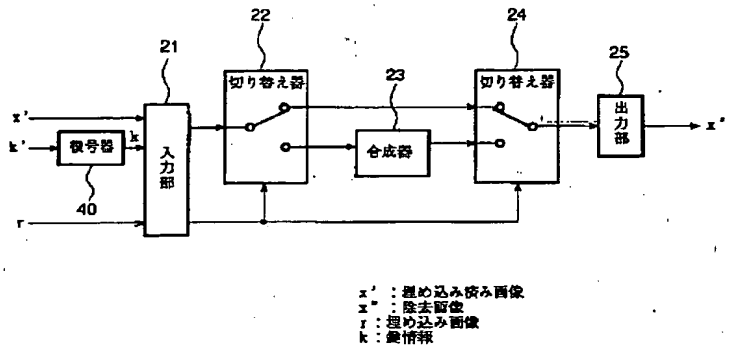
【 図9 】



【 図10 】

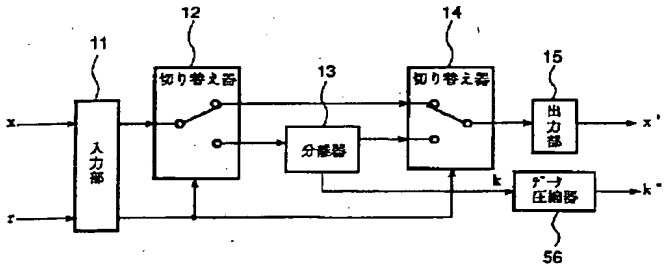
0	0	0	0	0	0	0	0	0	0	0	0
0	1	1	1	1	0	0	0	0	0	1	1
1	1	0	0	0	1	0	0	0	0	1	0
1	0	0	0	0	0	0	0	0	1	1	0
1	0	0	0	0	0	0	0	0	1	1	1
1	1	0	0	0	1	0	0	1	1	1	1
0	1	1	0	0	1	0	0	1	1	0	0
0	0	1	1	1	0	0	0	1	1	0	0

【 図4 】



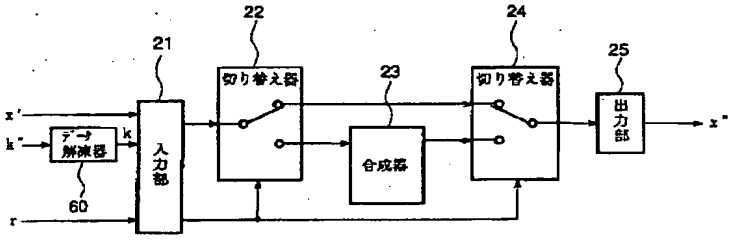
x' ：埋め込み済み画像
x" ：除去画像
r ：埋め込み画像
k ：鍵情報

【 図5 】



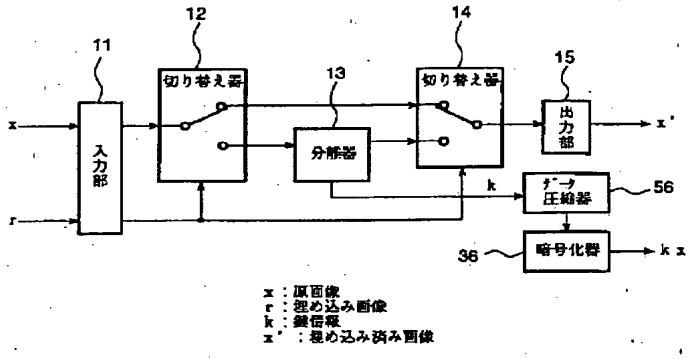
x ：原画像
r ：埋め込み画像
k ：鍵情報
x' ：埋め込み済み画像

【 図6 】

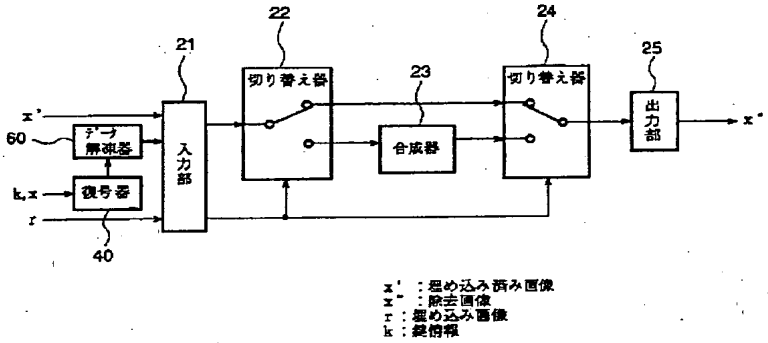


x' ：埋め込み済み画像
x" ：除去画像
r ：埋め込み画像
k ：鍵情報

【図7】



【図8】



フロントページの続き

Fターム(参考) 5B057 CA01 CA12 CA16 CB01 CB16
CE08 CE17 CG07
5C053 FA13 GA11 GB06 GB22 HA29
JA30 KA21 KA24 LA06
5C064 CA14 CB01 CC04
5C076 AA13 AA14 AA26 BA06
5J104 AA14 NA02 NA14 NA27